WHAT IS CLAIMED IS:

1. A method comprising:

defining a key and a set of values, the key being determined by the values and a predefined relationship,

sending one of the values of the set and information encrypted using the key to a server; and

sending another of the values of the set to a first delegate.

2. The method of claim 1 further comprising:

generating a second set of values, the key being also determined by the values of the second set;

sending one of the values of the second set to the server; and

sending another of the values of the second set to a second delegate.

3. The method of claim 2 in which the values of the second set are also determined by the predefined relationship.

4. The method of claim 1 in which the set includes exactly two values.

5. The method of claim 1 in which the set includes three or more values.

6. The method of claim 1 in which the value of the set sent to the server is associated with a descriptor of the first delegate.

7. The method of claim 1 in which the probability of guessing the key correctly using knowledge of one or more of the values of the set, but not all the values of the set is the same as the probability of guessing the key correctly using no knowledge of any value of the set.

8. The method of claim 7 in which the predefined relationship comprises the Boolean XOR function or a relationship that applies an encryption algorithm to one value of the set using another value of the set as the encryption algorithm key.

9. The method of claim 1 in which the information comprises medical information.

10. A method comprising:

storing, on a server accessible through a network, secured information and a first access component, use of the secured information requiring the first access component and a second access component; and

providing the secured information and the first access component to a first requestor.

11. The method of claim 10 in which the second access component is not stored on the server.

12. The method of claim 10 further comprising storing a third access component, such that the third access component and a fourth access component are sufficient to permit use of the secured information.

13. The method of claim 12 further comprising providing the secured information and the third access component to a second requestor.

14. The method of claim 12 further comprising deleting the third access component in response to a trigger, the trigger being a client instruction, a time limit, a request from the first requestor, or a security breach.

15. The method of claim 12 further comprising identifying the requestor and determining that the requestor requires the first access component but not the third access component.

16. The method of claim 10 further comprising storing permission information about the identity of a party approved for access, such that the secured information and the first access component are only provided if the first requestor is an approved party.

17. The method of claim 10 in which the secured information is secured by encryption using a key, and the first and second access components are related to the key by a predefined relationship.

18. A method comprising:

receiving

a) from a client, a first access component required for use of secured information, the use requiring the first access component and a second access component,

b) from a server accessible through a network, the secured information, and

c) from a source other than the client, the second access component.

19. The method of claim 18 in which the source is the server.

20. The method of claim 18 in which the source is other than the server.

21. The method of claim 18 in which a third access component is required in addition to the first and second access components for use of the secured information.

22. The method of claim 18 in which the secured information, the first access component, and the second access component are received in a digital form.

23. An article comprising a machine-readable medium that stores machine-executable instructions, the instructions causing a machine to:

define a key and a set of values, the key being determined by the values and a predefined relationship,

send one of the values of the set and information encrypted using the key to a server; and

send another of the values of the set to a first delegate.

24. The article of claim 23 in which the instructions further cause a machine to:

generate a second set of values, the key being independently determined by the values of the second set;

send one of the values of the second set to the server; and

send another of the values of the second set to a second delegate.

25. An apparatus comprising a processor and instructions configured to cause the processor to:

receive, from a client, information and a value of a set of values, the information being encrypted using a key, the key being determined by the values of the set and a predefined relationship;

store the information and the value, but not all the values of the set; and

transmit, to a delegate, the information and the value.

26. The apparatus of claim 25 in which the software is further configured to cause the processor to:

store a second value that is a member of a second set of values, the values of the second set being sufficient to determine the key using the predefined relationship.

27. The apparatus of claim 25 in which the software is further configured to cause the processor to:

delete or deny access to the second value in response to a trigger, the trigger being a client instruction, a time limit, a request from the delegate, or a security breach.

28. The apparatus of claim 25 in which the information comprises medical information.

29. A method comprising:

encrypting information using an encryption key;

sending the encryption key, but not the encrypted information to a first party;

sending the encrypted information, but not the encryption key to a server.

30. The method of claim 29 further comprising sending a descriptor of the first party to the server to thereby authorize the server to provide the encrypted information to the first party.